UNIVERSIDAD POLITÉCNICA DE

SAN LUIS POTOSÍ

CARRERA: Ingeniería en Tecnologías de la Información

MATERIA: Seguridad Informatica

TRABAJO: ACTIVIDAD 02: Análisis de servicios de seguridad (X.800 y RFC 4949)

PARCIAL 1

Aguilar Carrizales Miguel Angel / 182318

Fecha de entrega: 27 de Enero de 2026

Introducción

En este trabajo se revisarán distinto escenarios de ataques o vulnerabilidades que ocurrieron, que relación llevan con el ITU T x800 y el RFC 4949

Escenario 01. En múltiples incidentes atribuidos al grupo LockBit, organizaciones públicas y privadas han sufrido el cifrado masivo de servidores tras un acceso inicial no autorizado. Antes de ejecutar el ransomware, los atacantes exfiltraron información sensible y posteriormente amenazaron con su publicación, evidenciando un compromiso simultáneo de la confidencialidad, la integridad y la disponibilidad. Desde el enfoque del RFC 4949, el incidente se clasifica como un multi-stage attack con data breach y availability attack, donde la indisponibilidad del sistema es solo una fase final del daño. La ausencia de respaldos inmutables y de detección temprana permitió que el impacto fuera total.

Elemento	Respuesta
Servicios X.800 comprometidos	confidencialidad Propiedad de una información que no está disponible ni es divulgada a personas, entidades o procesos no autorizados. disponibilidad Propiedad de ser accesible y utilizable a petición por una entidad autorizada integridad de los datos Propiedad que garantiza que los datos no han sido alterados o destruidos de una manera no autorizada.
Definiciones aplicables RFC 4949	Availability Service Servicio de seguridad cuyo objetivo es garantizar que los sistemas, servicios y recursos de información permanezcan accesibles y operativos cuando son requeridos por los usuarios autorizados, incluso frente a fallos, ataques o interrupciones. Back up Proceso mediante el cual se crean copias de reserva de datos o se establecen mecanismos alternativos de operación, con el fin de asegurar la continuidad del sistema ante la pérdida, corrupción o indisponibilidad de recursos críticos.
Tipo de amenaza	Amenaza Externa
Vector de ataque	Exploit, Credenciales robadas
Impacto técnico/operativo	Cifrado de servidores, Pérdidad de datos sensibles, interrupción completa de operaciones, riesgo reputacional
Medida de control	Uso de backups, segmentación de red

Escenario 02. En diversos casos documentados, bases de datos completas quedaron accesibles públicamente debido a errores de configuración en servicios de almacenamiento en la nube. No existió una explotación técnica sofisticada, sino una falla en el control de acceso, lo que derivó directamente en la pérdida de confidencialidad de los datos. El RFC 4949 describe este tipo de incidentes como misconfiguration y exposure, subrayando que la amenaza no siempre implica malware o intrusión activa. El impacto suele ser legal y reputacional, aun cuando no se pueda demostrar acceso malicioso.

Elemento	Respuesta
Servicios X.800 comprometidos	confidencialidad Propiedad de una información que no está disponible ni es divulgada a personas, entidades o procesos no autorizados.
Definiciones aplicables RFC 4949	Misconfiguration exposure Tipo de acción de amenaza en la que información sensible es liberada o expuesta directamente a una entidad no autorizada, ya sea de forma intencional o accidental, comprometiendo la confidencialidad de los datos y violando la política de seguridad del sistema.
Tipo de amenaza	Interna
Vector de ataque	Acceso público sin autenticación, servivios en la nube mal configurados
Impacto técnico/operativo	Exposición de datos sensibles, problemas legales
Medida de control	Minimo privilegio, auditorías de seguridad

Escenario 03. Un proveedor legítimo de software fue comprometido y distribuyó una actualización que incluía código malicioso, afectando a cientos de organizaciones que confiaban en él. Este escenario refleja una violación grave de la integridad de los sistemas y, en muchos casos, de la confidencialidad, al permitir accesos no autorizados posteriores. El RFC 4949 lo identifica como supply chain attack, destacando el abuso de relaciones de confianza. El daño es particularmente crítico porque rompe el supuesto de legitimidad del software firmado.

Elemento	Respuesta
Servicios X.800 comprometidos	confidencialidad Propiedad de una información que no está disponible ni es divulgada a personas, entidades o procesos no autorizados. integridad de los datos

	Propiedad que garantiza que los datos no han sido alterados o destruidos de una manera no autorizada.
Definiciones aplicables RFC 4949	Trojan horse Programa que aparenta cumplir una función legítima, pero que contiene código oculto con fines maliciosos, el cual se ejecuta aprovechando la confianza del usuario o las autorizaciones válidas del sistema para evadir los mecanismos de seguridad. trust anchor Punto base de confianza, generalmente asociado a una autoridad certificadora u organización reconocida, desde el cual se inicia la validación de certificados y cadenas de confianza dentro de una infraestructura de clave pública
Tipo de amenaza	Externa
Vector de ataque	Actualización comprometida, código malicioso
Impacto técnico/operativo	APT, Perdida de confianza
Medida de control	Zero trust, validación de integridad y comportamiento

Escenario 04. Mediante campañas de phishing, atacantes obtuvieron credenciales válidas y accedieron a sistemas corporativos durante meses sin levantar alertas. Aunque la autenticación funcionó técnicamente, el servicio de autenticación fue comprometido al basarse en credenciales robadas, afectando también el control de acceso. Según el RFC 4949, se trata de un credential compromise con authentication failure conceptual, no técnica. La falta de MFA y de monitoreo de comportamiento facilitó la persistencia del atacante.

Elemento	Respuesta
Servicios X.800 comprometidos	Autenticación Estos servicios proporcionan la autenticación de una entidad par comunicante y de la fuente de datos, según se describe a continuación Control de acceso Este servicio proporciona protección contra el uso no autorizado de recursos accesibles mediante ISA. Estos recursos a los que se tiene acceso mediante protocolos de ISA, pueden ser o no de ISA. Este servicio de protección puede aplicarse a diversos tipos de acceso a un recurso (por ejemplo, el uso de un recurso de comunicaciones, la lectura,

	la escritura, o la supresión de un recurso de información; la ejecución de un recurso de procesamiento) o a todos los accesos a un recurso. confidencialidad Propiedad de una información que no está disponible ni es divulgada a personas, entidades o procesos no autorizados.
Definiciones aplicables RFC 4949	masquerade Tipo de amenaza en la que una entidad no autorizada se hace pasar por una entidad legítima para obtener acceso indebido a un sistema o ejecutar acciones maliciosas bajo una identidad falsa. Credential Elemento de información que vincula un identificador con datos de autenticación, y que permite verificar la identidad de una entidad que intenta acceder a un sistema, como contraseñas, tokens o certificados digitales.
Tipo de amenaza	Ingenieria Social
Vector de ataque	Phishing
Impacto técnico/operativo	Robo de información, sistema comprometido
Medida de control	MFA obligatorio, campaña de concientización

Escenario 05. En ataques de ransomware avanzados, los atacantes eliminaron o cifraron los respaldos antes de afectar los sistemas productivos. Este hecho compromete directamente la disponibilidad y la integridad de la información, al impedir la recuperación. El RFC 4949 clasifica este comportamiento como data destruction y availability attack, evidenciando intención deliberada de maximizar el daño. La inexistencia de respaldos offline o inmutables convierte el incidente en catastrófico.

Elemento	Respuesta
Servicios X.800 comprometidos	disponibilidad Propiedad de ser accesible y utilizable a petición por una entidad autorizada integridad de los datos Propiedad que garantiza que los datos no han sido alterados o destruidos de una manera no autorizada.

Definiciones aplicables RFC 4949	data compromise Incidente de seguridad en el cual la información queda expuesta a accesos no autorizados, existiendo la posibilidad de divulgación, modificación o uso indebido de los datos afectados.
Tipo de amenaza	Externa
Vector de ataque	Acceso privilegiado, Eliminación de respaldos
Impacto técnico/operativo	Interrupción parcial o total del negocio
Medida de control	Backups offline, Pruebas periodicas de restauración

Escenario 06. Un empleado con acceso legítimo extrajo bases de datos completas y las vendió a terceros, sin explotar vulnerabilidades técnicas. El servicio afectado fue principalmente la confidencialidad, junto con fallas en el control de acceso por exceso de privilegios. El RFC 4949 define este escenario como insider threat, destacando que el riesgo interno puede ser tan grave como el externo. La carencia de monitoreo y de políticas de mínimo privilegio fue determinante.

Elemento	Respuesta
Servicios X.800 comprometidos	Control de acceso Este servicio proporciona protección contra el uso no autorizado de recursos accesibles mediante ISA. Estos recursos a los que se tiene acceso mediante protocolos de ISA, pueden ser o no de ISA. Este servicio de protección puede aplicarse a diversos tipos de acceso a un recurso (por ejemplo, el uso de un recurso de comunicaciones, la lectura, la escritura, o la supresión de un recurso de información; la ejecución de un recurso de procesamiento) o a todos los accesos a un recurso confidencialidad Propiedad de una información que no está disponible ni es divulgada a personas, entidades o procesos no autorizados.
Definiciones aplicables RFC 4949	insider Persona que posee acceso legítimo a un sistema desde dentro de su perímetro de seguridad, y que, de manera intencional o accidental, puede representar un riesgo para la confidencialidad, integridad o disponibilidad de la información.
Tipo de amenaza	Interna

Vector de ataque	Uso indebido de accesos legitimos
Impacto técnico/operativo	Daño legal y reputacional. Fuga de información.
Medida de control	Minimo privilegio, Monitoreo de actividades.

Escenario 07. Tras un ataque, los registros del sistema quedaron cifrados o alterados, impidiendo reconstruir la secuencia de eventos. Esto compromete la integridad de los datos y el no repudio, ya que no es posible demostrar qué ocurrió ni quién fue responsable. Desde el RFC 4949, se trata de una violación de evidentiary integrity y del audit trail. El impacto no solo es técnico, sino también probatorio y legal.

Elemento	Respuesta
Servicios X.800 comprometidos	integridad de los datos Propiedad que garantiza que los datos no han sido alterados o destruidos de una manera no autorizada. 5.2.5.1 No repudio con prueba del origen Se proporciona al destinatario de los datos la prueba del origen de los datos. Esto lo protegerá contra cualquier tentativa del expedidor de negar que ha enviado los datos o su contenido.
Definiciones aplicables RFC 4949	audit trail Conjunto de registros que documentan las actividades realizadas dentro de un sistema, permitiendo reconstruir eventos, detectar incidentes y proporcionar evidencia para análisis forense o cumplimiento normativo.
Tipo de amenaza	Externa
Vector de ataque	Alteración de logs, acceso administrativo
Impacto técnico/operativo	Imposibilidad de análisis forense
Medida de control	SIEM, Logs inmutables

Escenario 08. Una actualización mal ejecutada provocó la caída simultánea de múltiples servicios críticos a nivel global. Aunque no existió un atacante, el servicio de disponibilidad fue gravemente afectado. El RFC 4949 contempla estos eventos como operational failure, recordando que la seguridad también se ve afectada por errores internos. La falta de pruebas previas y planes de reversión amplificó el impacto

Elemento	Respuesta

Servicios X.800 comprometidos	disponibilidad Propiedad de ser accesible y utilizable a petición por una entidad autorizada
Definiciones aplicables RFC 4949	operational integrity Condición que asegura que los sistemas no solo mantienen su integridad estructural, sino que además ejecutan correctamente sus funciones previstas, sin alteraciones no autorizadas que afecten su desempeño real.
Tipo de amenaza	Interno
Vector de ataque	Actualización defectuosa
Impacto técnico/operativo	Caida de servicios, perdidas económicas.
Medida de control	Plan de reversión, Pruebas en ambientes controlados

Escenario 09. Atacantes replicaron sitios y correos oficiales para engañar a ciudadanos y obtener información sensible. Este escenario afecta la autenticación, al suplantar identidades legítimas, y la confidencialidad de los datos recolectados. El RFC 4949 lo clasifica como masquerade y phishing, subrayando el componente de ingeniería social. La ausencia de mecanismos de autenticación del dominio y de concientización facilitó el éxito del ataque.

Elemento	Respuesta
Servicios X.800 comprometidos	Autenticación Estos servicios proporcionan la autenticación de una entidad par comunicante y de la fuente de datos, según se describe a continuación confidencialidad Propiedad de una información que no está disponible ni es divulgada a personas, entidades o procesos no autorizados.
Definiciones aplicables RFC 4949	masquerade Tipo de amenaza en la que una entidad no autorizada se hace pasar por una entidad legítima para obtener acceso indebido a un sistema o ejecutar acciones maliciosas bajo una identidad falsa. phishing Técnica de ingeniería social mediante la cual un atacante intenta obtener información sensible engañando a las víctimas, haciéndose

	pasar por una entidad legítima a través de correos electrónicos, sitios web o mensajes fraudulentos.
Tipo de amenaza	Ingenieria Social
Vector de ataque	Sitios web falsos, correos falsos
Impacto técnico/operativo	Robo de información, perdida de confianza
Medida de control	Concientización, certificados digitales

Escenario 10. En algunos incidentes, tras exfiltrar información, los atacantes ejecutaron acciones destructivas para borrar sistemas completos y eliminar rastros. Se produce un compromiso total de la confidencialidad, la integridad y la disponibilidad, configurando uno de los peores escenarios posibles. El RFC 4949 describe este patrón como destructive attack, donde el objetivo no es solo el lucro, sino el daño irreversible. La detección tardía impidió cualquier contención efectiva.

Elemento	Respuesta
Servicios X.800 comprometidos	confidencialidad Propiedad de una información que no está disponible ni es divulgada a personas, entidades o procesos no autorizados. disponibilidad Propiedad de ser accesible y utilizable a petición por una entidad autorizada integridad de los datos Propiedad que garantiza que los datos no han sido alterados o destruidos de una manera no autorizada.
Definiciones aplicables RFC 4949	attack Acción intencional dirigida a evadir los servicios de seguridad y violar la política de seguridad de un sistema, con el objetivo de comprometer sus activos mediante el uso de una amenaza deliberada.
Tipo de amenaza	Externa
Vector de ataque	Exfiltración seguida de acciones destructivas
Impacto técnico/operativo	Pérdida irreversible, Paralización de la empresa
Medida de control	Segmentación, plan de recuperación, detección temprana

Conclusión

Existen muchos tipos de escenarios en los que problemas, ataques o errores pueden comprometer la información, reputación o legalidad de distintas formas, haciendo el reporte recordé lo fácil que cualquiera puede tener problemas de ciberseguridad.

Al conocer más tipos de ataques se puede planear de manera más efectiva el evitar que ocurran o tener un plan de contingencia por si llegan a pasar.

Referencias

Shirey, R. W. (2007). *Internet Security Glossary, Version 2* (RFC 4949, Informational). IETF. https://doi.org/10.17487/RFC4949

International Telecommunication Union. (1991). *Security Architecture for Open Systems Interconnection for CCITT Applications* (ITU-T Rec. X.800).